456-TP-009-001

ECS Project Training Material Volume 9: System Troubleshooting

Technical Paper

May 1997

Prepared Under Contract NAS5-60000

RESPONSIBLE ENGINEER

Paul E. Van Hemel Date
EOSDIS Core System Project

SUBMITTED BY

Tom Hickey, M&O Deputy Manager Date
EOSDIS Core System Project

Hughes Information Technology Systems
Upper Marlboro, Maryland

This page intentionally left blank.

Abstract

This is Volume 9 of a series of 10 volumes containing the training material for the Pre-Release B Testbed of the Earth Observing System Data and Information System (EOSDIS) Core System (ECS). This lesson provides a detailed description of the different tasks that are required to perform software maintenance. The lesson includes a detailed review of the system monitoring capabilities, troubleshooting process, and trouble ticket set-up and processing.

***Keywords**:* training, instructional design, course objective, system troubleshooting, trouble ticket, maintenance

This page intentionally left blank.

Contents

Abstract

Introduction

Identification 1

Scope 1

Purpose 1

Organization 1

System Troubleshooting Overview

Lesson Overview 3

Lesson Objectives 3

Importance 4

System Performance Monitoring

Checking the Health and Status of the Network 5

- Starting and Ending a NNM Session 6
- Looking at maps for color alerts 9
- Looking at maps for new nodes 10
- Creating special submaps for monitoring status 11
- Checking for event notifications 13

Accessing the EOSDIS Backbone Network (EBnet) Web Page 14

Problem Analysis/Troubleshooting

Analysis/Troubleshooting: System 17

Analysis/Troubleshooting: COTS Hardware 18

Performing Preventive Maintenance 21

Trouble Ticket (TT)

Using Problem Report Software 23
Modifying DDTS Configuration and Privileges 23
Adding Users to DDTS 28
Performing Operational Work-around 30

Diagnosing Network Communications Problems

Identifying Network Connectivity Problems 31
Identifying Network Performance Problems 34
Diagnosing Network Service Problems 36
Viewing Historical Trends 38
Establishing Baselines for Normal Network Performance 38
Building Applications to Monitor Trends 40
Refining Thresholds 45
Setting Up Event-Triggered Actions 46
Using the Event History Log Browser 47

Practical Exercise

Perform Activities Related to System Monitoring and Troubleshooting 49

Slide Presentation

Slide Presentation Description 51

Figures

1 Example of Network Map Screens from HP OpenView 6
2 HP OpenView Default Status Colors 8
3 HP OpenView Event Categories Window 13
4 EBnet Home Page 16
5 Example of HP OpenView Graphical Display of CPU Usage 35

Introduction

Identification

Training Material Volume 9 is part of a series of Technical Papers that will be used to teach Maintenance and Operations (M&O) concepts to the M&O staff at the following Distributed Active Archive Centers (DAACs): Langley Research Center (LaRC), National Snow and Ice Data Center (NSIDC), and EROS Data Center (EDC).

Scope

Training Material Volume 9 describes the process and procedures for ECS System Troubleshooting. This lesson is designed to provide the operations staff with sufficient knowledge and information to satisfy all lesson objectives.

This document reflects the August 23, 1995 Technical Baseline maintained by the contractor Configuration Control Board (CCB) in accordance with ECS technical direction #11, dated December 6, 1994.

Purpose

The purpose of this Technical Paper is to provide a detailed course of instruction that forms the basis for understanding System Troubleshooting Lesson objectives are developed and will be used to guide the flow of instruction for this lesson. The lesson objectives will serve as the basis for verifying that all lesson topics are contained within this Student Guide and slide presentation material.

Organization

This document is organized as follows:

Introduction:	The Introduction presents the document identification, scope, purpose, and organization.
Student Guide:	The Student Guide identifies the core elements of this lesson. All Lesson Objectives and associated topics are included.
Slide Presentation:	Slide Presentation is reserved for all slides used by the instructor during the presentation of this lesson.

This page intentionally left blank.

System Troubleshooting Overview

Lesson Overview

This lesson will provide you with the process for system/performance monitoring, problem analysis and troubleshooting of system hardware and software, managing the trouble ticket system, and diagnosing network communications problems. It provides practical experience in using the tools you will need for resolving system problems and minimizing system down time.

Lesson Objectives

Overall Objective - The overall objective of this lesson is proficiency in the methodology and procedures for system troubleshooting of the Earth Observing System Data and Information System (EOSDIS) Core System (ECS).

Condition - The student will be given a workstation console with access to ECS software tools including Trouble Ticket, Fault/Performance Management, HP OpenView, and Management Services Subsystem (MSS) graphical user interface (GUI) tools.

Standard - The student will use the tools in accordance with prescribed methods and complete required procedures without error.

Specific Objective 1 - The student will conduct system performance monitoring, to include checking the health and status of the network and accessing the EOSDIS Backbone Network (EBnet) Web Page.

Condition - The student will be given a workstation console with access to HP OpenView.

Standard - The student will use HP OpenView in accordance with specified procedures and without error to examine maps for color alerts and new nodes, create special submaps for monitoring status, and check for event notifications.

Specific Objective 2 - The student will perform problem analysis and troubleshooting, to include analysis and troubleshooting of the system, analysis and troubleshooting of commercial off-the-shelf (COTS) hardware, and preventive maintenance.

Condition - The student will be given a workstation console with access to ECS software tools including Trouble Ticket, Fault/Performance Management, HP OpenView, and Management Services Subsystem (MSS) graphical user interface (GUI) tools.

Standard - The student will use the GUI tools without error in accordance with applicable procedures to perform the required troubleshooting and maintenance activities.

Specific Objective 3 - The student will perform the functions required to set up and manage trouble ticket processing, including administrative set-up of projects, users, and privileges in the Testbed trouble ticket software (DDTS).

Condition - The student will be given a workstation console with access to ECS software tools including Trouble Ticket, Fault/Performance Management, HP OpenView, and Management Services Subsystem (MSS) graphical user interface (GUI) tools.

Standard - The student will use the GUI tools without error in accordance with applicable procedures to perform the required trouble ticket functions.

Specific Objective 4 - The student will perform the functions required to diagnose network communications problems.

Condition - The student will be given a workstation console with access to ECS software tools including Fault/Performance Management, HP OpenView, and Management Services Subsystem (MSS) graphical user interface (GUI) tools.

Standard - The student will use the GUI tools without error in accordance with applicable procedures to perform the required troubleshooting/diagnosis of network communications problems.

Importance

This lesson provides students with the knowledge and skills needed for effective system troubleshooting and maintenance of the ECS. It is structured to provide useful skills and knowledge concerning ECS operation and the tools for identifying system problems and returning malfunctioning system hardware and software to normal operational status. It provides useful instruction and practical exercises in maintaining ECS in an operationally ready condition, and is therefore vital to students who are preparing for a number of different positions with responsibilities in maintaining that system readiness, including positions as:

- Computer Operator, System Administrator, and Maintenance Coordinator at the DAAC.
- System Engineer, System Test Engineer, System Administrator, and Software Maintenance Engineer at the Sustaining Engineering Organization (SEO)..
- System Engineer, System Test Engineer, and Maintenance Engineer at the DAAC.

System Performance Monitoring

The key to maintaining ECS in an operationally ready state is effective performance monitoring.

- System operators – close monitoring of progress and status of system and subsystem functions that are the focus of their jobs.
  - Notice any serious degradation of system performance that has an impact on their abilities to conduct their jobs successfully and meet user needs.
- System administrators and system maintenance personnel – monitor overall system functions and performance.
  - Administrative and maintenance oversight of system.
  - Watch for system problem alerts.
  - Use monitoring tools to create special monitoring capabilities.
  - Check for notification of system events.

Checking the Health and Status of the Network

ECS is heavily dependent on the use of computer networks. HP OpenView is a management tool that provides operators and maintainers with a system view for monitoring and checking the network, for quickly identifying parts of the network that may have problems, and for isolating faults on the network. It provides the following general features:

- a site-wide view of network and system resources.
- status information on resources.
- event notifications and background information.
- operator interface for managing resources.

Specific monitoring capabilities provided by HP OpenView Network Node Manager (NNM) include:

- a network map with color alerts to indicate problems.
- indication of network changes.
- creation of submaps for special monitoring.
- event notifications.

Figure 1 shows an example of Testbed network map screens from HP OpenView.

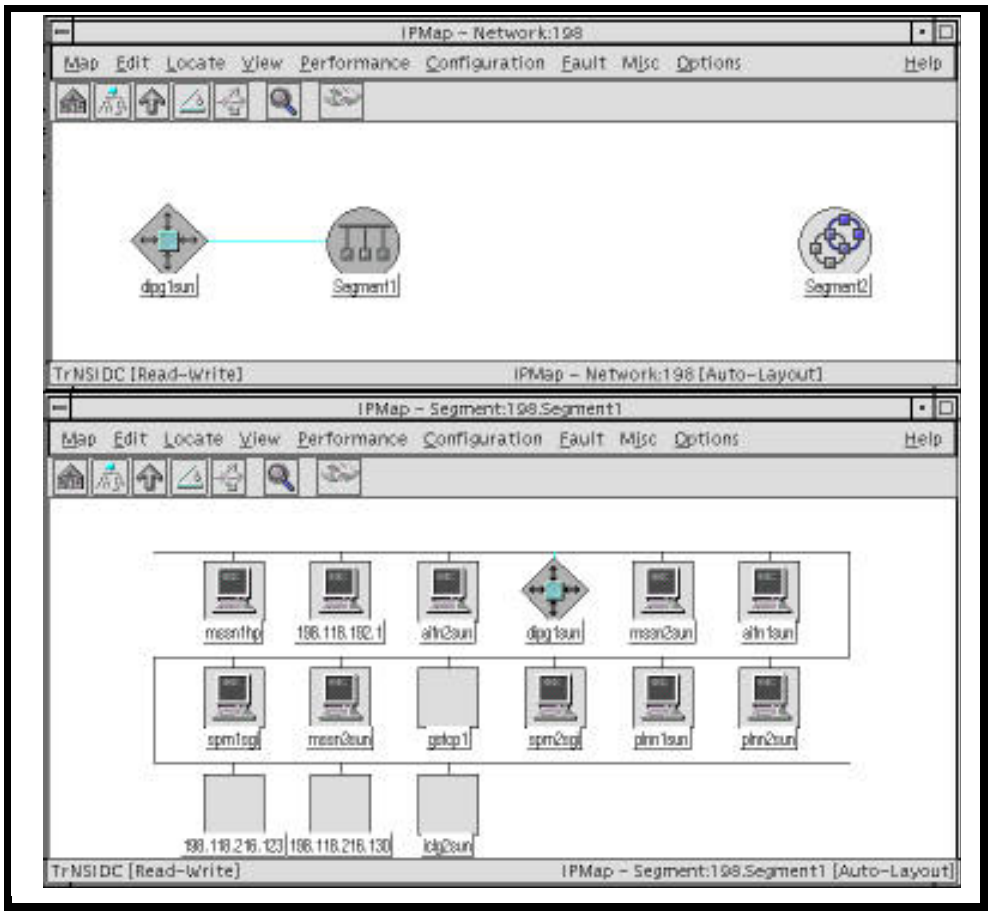


Figure 1. Example of Network Map Screens from HP OpenView

HP OpenView is capable of discovering a network and its elements. To use HP OpenView NNM to monitor the network, it must be running and configured to display status, with its Network map set for read-write and the Internet Protocol (IP) map enabled.

Starting and Ending a NNM Session

For NNM to report properly on the network topography, HP OpenView Windows (OVW) must be activated. Once activated, OVW automatically starts NNM, as well as any installed and registered NNM applications. As a prerequisite, the network management processes that work with OVW and NNM must be running. These network management processes are:

- **ovwdb** - the process that maintains the OVW database.
- **trapd** - the process that multiplexes and logs SNMP traps.
- **ovtopmd** - the process that maintains the network topology database.
- **ovactiond** - the process that executes commands upon receipt of an event.
- **snmpCollect** - the process that collects MIB data and performs threshold monitoring.

- **netmon** - the process that polls SNMP agents for initial discovery of the network topology and for detecting changes in the network topology, configuration, and status.

To see if these processes are running, type **/usr/OV/bin/ovstatus** at a UNIX prompt on the HP OpenView server.

To perform the start-up, use the following procedure.

Start the HP OpenView Windows NNM Graphical User Interface

1 On workstation **mss*x*#hp**, at the UNIX prompt in a terminal window, type **/usr/OV/bin/ovstatus** at a UNIX command prompt and then press the **Return** key.

- NOTE: The ***x*** in the workstation name will be a letter designating your site: **g** = GSFC, **l** = LaRC, **e** = EDC, and **n** = NSIDC (e.g., **mssn1hp** indicates a management services subsystem *hp* workstation at NSIDC). If you access the workstation through a remote login (rlogin), you must enter **xhost +** prior to the rlogin, and enter **setenv DISPLAY <local_workstation IP address>:0.0** after the rlogin before entering the **ovstatus** command.
- A series of messages is displayed indicating for each process that its state is "**RUNNING**" or "**NOT_RUNNING**."
- If the network management processes are not running, a system administrator (logged in as **root**) can start them by typing **/usr/OV/bin/ovstart** and then pressing the **Return** key.

2 Type **/usr/OV/bin/ovw &** and press the **Return** key.

- The **About OVW** box is displayed, followed in a few moments by the OVW submap window, and any installed and registered NNM applications are also started.
- The **Event Categories** window is displayed in the upper right corner of the screen.

To exit NNM and all other integrated applications, use the following procedure.

Exit NNM

1 From the menu bar on any submap window, follow menu path **Map→Exit**.

[or]

2 Click on the **Close** button on all open submap windows until the **Root** window is displayed. Then click on the **Close** button () on the **Root** window.

- The open map is saved and all submap windows and dialog boxes of the map are closed. OVW, all NNM applications, and all other integrated applications exit.

If you are logged in with HP OpenView NNM running you can get a quick assessment of the health and status of the network by checking the network map for color alerts. The symbols and the connections between them on the network map are color-coded to indicate status. There are two status categories:

- administrative – not propagated from child to parent through the network.
- operational – propagated from child to parent to indicate problems.

If the compound status (how status is propagated) for the open map is set to Default, the interpretation of the colors is as indicated in the table that appears in Figure 2. Note: If you have a color vision weakness, it is possible to change the colors displayed by HP OpenView. If you change them, make sure everyone who will use the software is aware of the changes.

Status Condition	Symbol Color	Connection Color
Unmanaged (a)	Off-white	Black
Testing (a)	Salmon	Salmon
Restricted (a)	Tan	Tan
Disabled (a)	Dark Brown	Dark Brown
Unknown (o)	Blue	Black
Normal (o)	Green	Green
Warning (o)	Cyan	Cyan
Minor/Marginal (o)	Yellow	Yellow
Major (o)	Orange	Orange
Critical (o)	Red	Red

(a) Administrative Status (o) Operational Status

Figure 2. HP OpenView Default Status Colors

Looking at maps for color alerts

To check your network for color alerts, you must first have the map for the network open. To open a map, use the following procedure:

Open a Network Map

1 With HP OpenView NNM running, follow menu path **Map→Maps→Open/List . . .**.

- The **Available Maps** dialog box is displayed.

2 Select the name of the map you want to open and click on "**Open Map**".

- A confirmation box is displayed.

3 Click on "**OK**".

- Any open map and its submap windows and dialogs close.
- The **Home Submap** (**Root**) of the selected map is displayed.

If you do not know the compound status scheme of the open map, follow the menu path **File→Describe/Modify Map** to obtain the **Map Description** dialog box and display/set the compound status scheme for default. Suppose there is a fault in an interface card in one of the workstations on your network. Use the following procedure to trace it using color alerts.

Looking at Maps for Color Alerts

1 Double click on the yellow **Internet** symbol.

- *Note*: The symbol will be yellow because the *critical* failure of the card in the workstation is propagated up to the level of the **Internet** symbol as a *minor* problem at that level.
- The **Internet submap** opens and displays the IP network(s). One IP network symbol is yellow. This indicates a marginal problem with the network.

2 Double click on the yellow **IP network** symbol.

- A **Network submap** opens and displays the Testbed segment(s) attached to the gateway(s). The segment symbol is yellow. This indicates a problem somewhere on the segment.

3 Double click on the yellow **segment** symbol.

- A **Segment submap** opens and displays the nodes attached to that segment. Of all the nodes in the segment, the workstation node is red. The problem is isolated to that workstation.

4 Double click on the red **workstation** symbol.

- A **Node submap** opens and displays its interface symbol. It is red.
- You have isolated the fault to a single card of a single node on your internet.

Looking at maps for new nodes

HP OpenView Windows includes an application called **IP Map** which, in default, is started automatically upon activation of HP OpenView Windows. IP Map creates network maps and submaps through several functions:

- automatically discovers all IP-addressable nodes on the network.
- creates an object for each discovered node.
- creates and displays symbols on the network map to represent created objects.
- creates a hierarchy of submaps to display the network in increasing detail.
  - internet submap.
  - network submaps.
  - segment submaps.
  - node submaps.

Each submap is assigned a layout algorithm that determines how its symbols are displayed. You can set automatic layout *on* or *off* to enable or disable enforcement of the layout algorithm, either for all submaps or for an individual submap. If autolayout is enabled, IP Map places new symbols directly on the submap. If autolayout is disabled, IP Map places new symbols in a **New Object Holding Area** in the lower part of the submap window. Symbols in the New Object Holding Area are shown without any connections. You can use HP OpenView to identify any new objects that are discovered and added to the open map. Suppose, for example, that a new workstation is added to the network and you wish to locate it and check its status. Use the following procedure to look for new nodes.

Looking at Maps for New Nodes

1 To check the default **Segment submap** for any new nodes that may have been discovered, open the default **Segment submap** from the segment symbol in the Network submap.

- View the submap for any new symbols.

2 To easily see new symbols in the submap, disable autolayout for the submap by following menu path **View→Automatic Layout→Off for this Submap**.

- When autolayout is disabled, a **New Object Holding Area** appears at the bottom of the submap.
- All newly added symbols are placed in the **New Object Holding Area**.

Creating special submaps for monitoring status

You can create submaps based on a logical organization rather than a physical one, to facilitate specialized monitoring. For example, suppose you want to have a submap just showing the Science Software Integration and Test (SSI&T) workstations at your site to have ready access to a display showing their status. Suppose further that you expect to use this submap frequently and therefore wish to create it within an existing hierarchy and be able to open it from a symbol in the Internet submap. Use the following procedure to create a special submap showing these workstations.

Creating Special Submaps for Monitoring Status

1 Decide where to locate your submap and whether it will have a parent or not.

- A submap without a parent object is independent of other existing submap hierarchies in the open map, and can be opened only from the **Available Submaps** dialog box. You can create child submaps of this submap, thereby creating a new submap hierarchy in the map.
- A submap that has a parent object can be opened from an explodable symbol of the parent object. If you want the new submap to exist within an existing submap hierarchy, you should create this submap from an explodable symbol.

2 To create a submap within an existing hierarchy, decide which symbol to use to open the new submap.

- If other symbols on the parent submap already open into child submaps or execute applications, you must create a new symbol to open the submap.

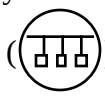
3 If you decide to create a new symbol (as in this case), add a symbol (for an existing object – in this case, a segment) or a new symbol and object to the submap of your choice (in this case, the Internet submap), by following menu path **Edit→Add Object . . .** .

- The **Add Object: Palette** window is displayed.

4 Click on the symbol representing the class of objects you want to add to the submap, using the scroll bar if necessary to scroll to the right for access to the desired symbol.

- For this training exercise, use the **Network Class**.
- The object symbols in the chosen class appear in the **Symbol Subclass** area of the **Add Object: Palette**.

5 Using the middle mouse button, drag the symbol representing the object to be added and drop it in the submap where it is to be added.

- You may add any of the symbols in the network class. For this training exercise, use the **bus** symbol ().
- The **Add Object** dialog box is displayed.

6 In the **Selection Name** field of the **Add Object** dialog, type a label for the object (e.g., for this training exercise, type **SSI&T Workstations** and then click on the **OK** button.

- The entered label appears on the newly added blue symbol.

7 Open the new submap by double-clicking on the newly created symbol and then clicking on the **OK** button in the **Question** dialog that appears. Copy SSIS&T Workstation objects from other submaps into the newly created map, following menu path **Edit→Copy** and **Edit→Paste** operations.

- For more information about these operations, see the *HP OpenView Windows User's Guide*.

8 If desired, for each workstation copied, add its connection by following menu path **Edit→Add Object . . . .**

- An **Add Connection** dialog is displayed, allowing you to select a type of connection (e.g., **Generic**), and then directing you to select a source and destination for the connection. You must then enter a selection name for the connection.
- When you click on **Close** for the **Add Connection** dialog, the newly added symbol changes color to indicate the status of its contained objects.

Checking for event notifications

Whenever a change occurs on the network, an **event** is generated. The occurrence of the event has two consequences:

- Through the internal processors of the **Network Node Manager**, the event is registered in a predefined category for display in an **Events Browser** window.
- The registration in the Events Browser window triggers a change for display in an **Event Categories** window (see Figure 3) to provide a notification that an event has occurred in the category of that Events Browser window. The display is a color change in a button on the Event Categories window corresponding to the event category. The color of the button indicates the highest severity event in the category. The default categories included in the Event Categories window are:
  - *Error Events*. This indicates inconsistent or unexpected behavior.
  - *Threshold Events*. This indicates that a threshold was exceeded.
  - *Status Events*. This indicates that an object or interface status changed to "up" or "down," or an object or interface started or stopped responding to Internet control message protocol (ICMP) echo requests.
  - *Configuration Events*. This indicates a node's configuration changed.
  - *Application Alert Events*. This indicates an HP OpenView Windows application generated an alarm or alert.
  - *All Events*. This indicates one or more of the previously listed events occurred. Selecting this button lists all events in the listed categories and others in one dialog box.

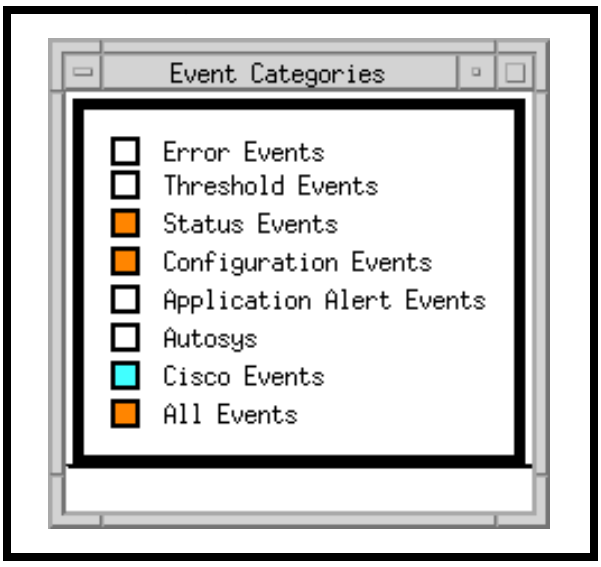


Figure 3. HP OpenView Event Categories Window

To check for event notifications, examine the Event Categories window to observe any color change in one or more of the buttons for the event categories. If there is a color change, you can click on the button to view its associated Events Browser window. For example, suppose you are monitoring the network when a critical threshold is exceeded somewhere on the network. Use the following procedure to check for event notifications.

Checking for Event Notifications

1 Observe that the **Threshold Events** button in the **Event Categories** window is red.

- This indicates that a critical threshold was exceeded somewhere on the network.

2 Click on the **Threshold Events** button in the **Event Categories** window. The **Threshold Events Browser** dialog box appears with a chronological listing of the threshold events that have occurred, with the most recent events at the bottom of the list.

- Each event listed includes the severity, time the event occurred, node on which the event occurred, and a brief event message.

3 To view the node that generated the event shown in this example, select the event from the list and click on **Action→Highlight Source on Map**.

- A map appears with the **busynode** node highlighted. At this point, select the highlighted node by clicking on it, and invoke appropriate operations from the menu bar to further diagnose and correct the situation which caused the threshold to be exceeded.

4 To delete the event, select the event and click on **Action→Delete→Selected Event**.

- This deletes only the selected event. (Note: multiple events may be selected and deleted.)
- For more information about event notification, click on the **help** button in the dialog box for the event being viewed or select **View SNMP Events** from the **Help: Index→Task**.

Accessing the EOSDIS Backbone Network (EBnet) Web Page

The EBnet is a Wide Area Network (WAN) that provides, in combination with other institutional and public networks, connectivity between geographically distributed EOSDIS facilities to support ECS mission operations and data production functions. Specifically, its functions include:

- provides connectivity between the ECS DAACs, the EOS Data and Operations System (EDOS) facilities, affiliated data centers, and other designated EOSDIS sites.
- serves as the interface between EDOS, the DAACs, and the NASA Science Internet (NSI).
- transporting spacecraft command, control, and science data nationwide on a continuous basis, 24 hours a day, 7 days a week.

- transports real-time mission-critical data related to the health and safety of on-orbit space systems and raw science telemetry as well as pre-launch testing and launch support.
- transports science data collected from spacecraft instruments and various levels of processed science data including expedited data sets, production data sets, and rate-buffered science data.
- provides wide-area communications through common carrier circuits for internal EOSDIS communications.
- interface to Exchange Local Area Networks (LANs) which provide communications between the WAN and site-specific LANs.

The NASA Communications (Nascom) organization at Goddard Space Flight Center (GSFC) maintains a home page for the EBnet (see Figure 4) on the World Wide Web at the following Universal Resource Location (URL):

- http://skynet.gsfc.nasa.gov/EBNET/EBnet.html.

This web site provides an overview of the EBnet as well as current data on its status and performance. Consequently, it can be a useful source of information when you are monitoring system performance. To access the EBnet Web Page, use the following procedure.

Accessing the EOSDIS Backbone Network (EBnet) Web Page

1 On workstation **mss*x*#hp**, at the UNIX prompt in a terminal window, type **Netscape** at a UNIX command prompt and then press the **Return** key.

- NOTE: The ***x*** in the workstation name will be a letter designating your site: **g** = GSFC, **l** = LaRC, **e** = EDC, and **n** = NSIDC (e.g., **mssn1hp** indicates a management services subsystem *hp* workstation at NSIDC). If you access the workstation through a remote login (rlogin), you must enter **xhost +** prior to the rlogin, and enter **setenv DISPLAY <local_workstation IP address>:0.0** after the rlogin before entering the **Netscape** command.
- The starting page selected to appear on launch of the browser is displayed.

2 Click on the **Location** window of the starting page.

- The contents of the **Location** window are highlighted.

3 Enter **http://skynet.gsfc.nasa.gov/EBNET/EBnet.html** in the **Location** window.

4 Press the **Return/Enter** key on the keyboard.

- The EOSDIS Backbone Network (EBnet) home page is displayed.

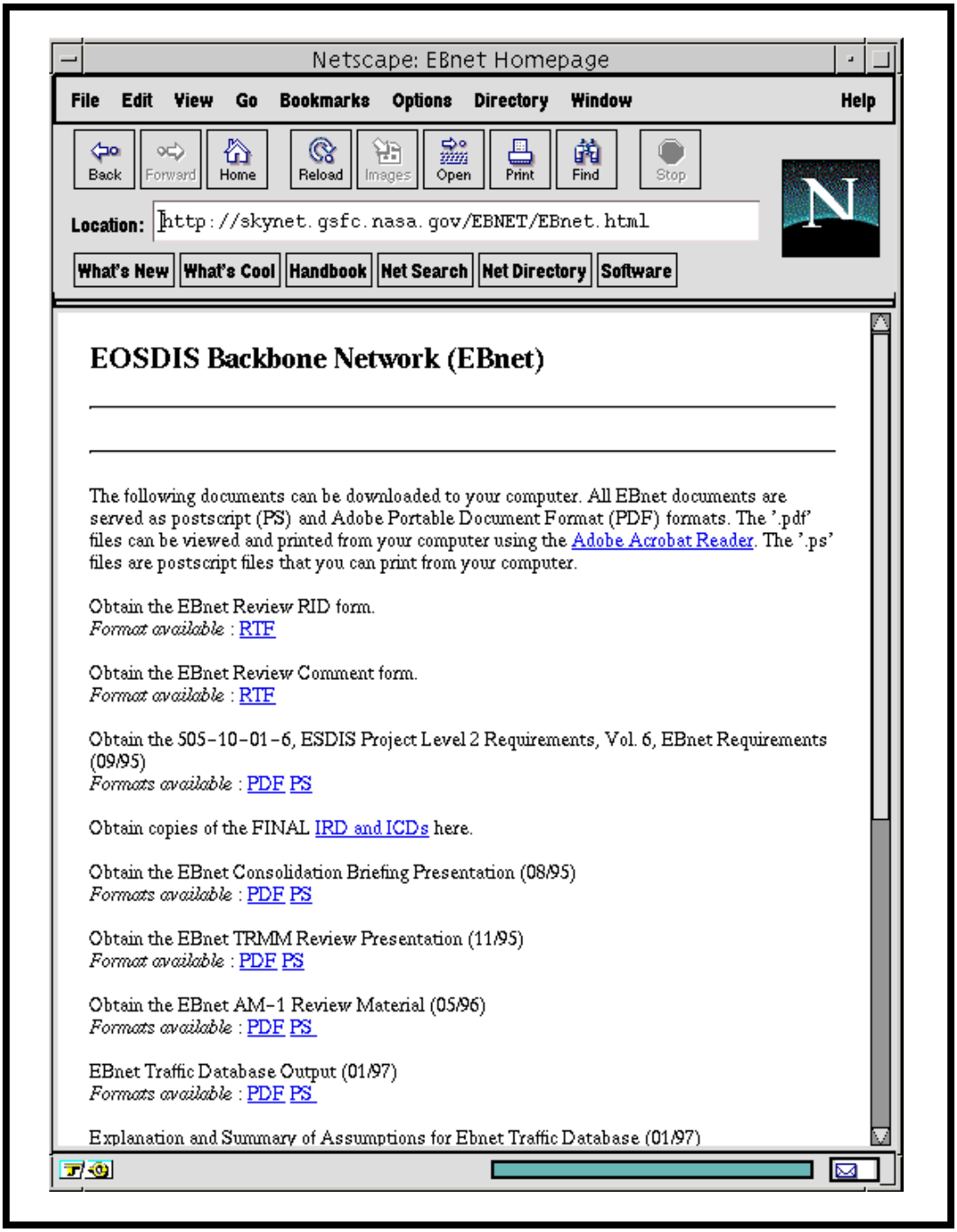


Figure 4. EBnet Home Page

Problem Analysis/Troubleshooting

Although ECS is designed to be a robust computer network system, the complexity of its hardware and software components and interfaces provides a wealth of potential sources for system failures or other non-conformance problems. Fortunately, the tools available in ECS provide several avenues of assistance to help you detect and isolate problems in the system.

Analysis/Troubleshooting: System

Some of the Commercial Off-The Shelf (COTS) software products that are part of ECS provide alerts or warnings when there are system problems. For example,:

- HP OpenView.
  - color alerts to indicate problems.
- AutoSys/Xpert.
  - color/auditory alerts to indicate job status/failures.

Many of the COTS products as well as the software developed specifically for ECS generate error messages and event messages to indicate errors and status. Several products also generate logs to capture and provide more detailed information about indicated problems. For example,:

- HP OpenView.
  - event notifications/events browser; focus on all system events.
- ClearCase®.
  - software installation error log files.

As is ever the case with a complex system, the effectiveness of troubleshooting depends on knowledge of the system and its documentation, applied systematically to diagnose problems. Your knowledge and skill may be called upon only after a user or an operator has already attempted some problem solving (e.g., based upon error messages displayed directly to the screen) and then submitted a trouble ticket. The effectiveness of your troubleshooting is maximized by:

- thorough documentation of the problem.
  - date/time of problem occurrence.
  - hardware/software.
  - initiating conditions.
  - symptoms.

- verification.
  - identify/review relevant publications (e.g., COTS product manuals, ECS tools and procedures manuals).
  - replicate problem.
- identification.
  - review product/subsystem logs.
  - review HP OpenView Event Browser.
- analysis.
  - detailed event review (e.g., HP OpenView Event Browser Event Fields).
  - determination of cause/action.

Analysis/Troubleshooting: COTS Hardware

The ECS hardware is composed almost entirely of commercial, off-the-shelf (COTS) products, for which there are vendor maintenance warranties and/or COTS hardware support contracts. When a system problem is discovered, there is an initial troubleshooting/diagnostics procedure to be followed which is generic – i.e., not limited to hardware problems. However, when a hardware problem is indicated, the procedure refers the problem to the Maintenance Coordinator for hardware corrective maintenance. System troubleshooting tools and principles apply:

- HP OpenView for quick assessment of status.
- HP OpenView Event Browser for sequence of events.
- Initial troubleshooting.
  - Review error message against hardware operator manual; prepare trouble ticket.
  - Verify connections (power, network, interface cables).
  - Run internal systems and/or network diagnostics.
  - Review system logs for evidence of previous problems.
  - Attempt system reboot.
  - If problem is hardware (e.g., software has been working and reboot is unsuccessful), report it to the Maintenance Coordinator – i.e., forward the trouble ticket.

A problem that is not resolved through initial troubleshooting will often require troubleshooting teamwork by the Maintenance Coordinator, the System Administrator, and perhaps a Network Analyst. These troubleshooters may perform additional steps to resolve the problem:

- specific troubleshooting procedures described in COTS hardware manuals.
- non-replacement intervention (e.g., adjustment).

- replace hardware with maintenance spare.
  - locally purchased (non-stocked) item.
  - installed (hot-swappable, excess capacity) spares (e.g., RAID storage, power supplies, network cards, tape drives).

If the hardware problem is not resolved by the actions of the local staff, it may be necessary to request assistance through the Maintenance Coordinator from a maintenance contractor for on-site hardware support. Suppose, for example, that you are a Maintenance Coordinator and HP OpenView has indicated a problem with one of the Sun workstations, that initial troubleshooting finds the workstation to be inoperable, that a trouble ticket has been forwarded to you, and that you and System Administrator are not able to resolve the problem through additional troubleshooting. That workstation is hard down. The correct approach is:

- Organize the data on the problem, find data on the appropriate support provider, and update the trouble ticket with this information.
- Call the support provider's technical support center to obtain on-site assistance.
  - Provide them with the background data.
  - Obtain a case reference number from them.
  - Update the trouble ticket to reflect the time and date of the call and the case number.
  - Notify the originator of the problem that the contractor is on the way.
- Arrange for site access for the maintenance technician.
  - Record arrival time.
  - Escort technician to hardware.
  - Assist in problem resolution (e.g., arrange equipment shutdown, demonstrate problem).
  - Obtain any needed technical references that are available at the site.
- Update trouble ticket with actions taken to correct the problem and delay time experienced for the repair, including start/stop times and reasons for each delay
- For any replaced part, update the trouble ticket with additional supporting data.
  - Part number of the new item.
  - Serial numbers of the old and new items.
  - Equipment Identification Number (EIN) assigned to the new item (if applicable).

- Model number of replacement Line Replaceable Unit (LRU). [Note: If the model number of the replacement LRU is different from the part removed, a configuration change request (CCR) is required for configuration management.]
- Name of the item replaced.

In preparation to request on-site hardware support from the maintenance contractor to repair the down Sun workstation, use the following procedure to obtain the background information needed.

Obtaining On-Site Hardware Support: Background Information

1 Collect information needed to obtain contract maintenance support.

- Obtain **make**, **model**, **serial number**, and **location** of the failed system from the hardware database.
- Obtain description of problem and symptoms from **trouble ticket**.
- Identify the **criticality** of the COTS hardware experiencing the problem.

2 Determine maintenance provider data.

- Obtain **name**, and **telephone number** of the maintenance provider.
- Obtain **access code** needed to obtain support.
- Obtain **telephone number** of the support provider's technical support center.
- Obtain **name** of site authorized contact person.

3 Record data on maintenance needed and maintenance provider into the trouble ticket.

In unusual cases, it may be necessary to resort to non-standard hardware support procedures. In the event that the maintenance contractor's assigned technician is not providing timely successful repair, or if the maintenance action is otherwise unsatisfactory, it may be necessary to escalate the problem to bring it to the attention of the support contractor's management. The escalation is achieved by calling the maintenance contractor's technical support center and providing them with the case reference number. Another non-standard support approach, which may be costly and is to be used only as a last resort for mission-critical repairs, is Time and Material (T&M) support. For T&M support, the local Maintenance Coordinator must obtain authorization from the ILS Maintenance Coordinator or, if that person is unavailable, from the System Monitoring and Coordination Center (SMC).

Performing Preventive Maintenance

For the initial release, the only hardware that requires scheduled preventive maintenance is the E-Systems Modular Automated Storage Systems (EMASS) robot.

- Scheduled by the local Maintenance Coordinator.
- Coordinated with maintenance organization and using organization.
  - Scheduled to be performed by maintenance organization and to coincide with any corrective maintenance if possible.
  - Scheduled to minimize operational impact.
- Documented using a trouble ticket.

This page intentionally left blank.

Trouble Ticket (TT)

We have seen that a system problem is typically documented using the DDTS COTS software product to prepare and update a problem report or trouble ticket (TT). Because there is a separate lesson that covers writing a trouble ticket, documenting changes, preparing and processing a trouble ticket through the Failure Review Board, and making emergency fixes, these topics are not addressed in detail here. By now you are familiar with the requirements for using trouble tickets in ECS problem management. You know that it is important to remember that high priority issues must be reviewed by the Failure Review Board (FRB), and that troubleshooting and repair activities that involve changes to the system configuration require a configuration change request (CCR).

Using Problem Report Software

Although you are familiar with using DDTS to create and view trouble tickets, there are other functions associated with the maintenance and operation of the trouble ticket service that you may be required to manage as a System Administrator or other manager. Specifically, the following tasks associated with DDTS may be required of the indicated administrator or others:

- modifying the DDTS configuration and controlling or changing privileges in DDTS.
- adding users to DDTS.

Let's look at each of these functions.

Modifying DDTS Configuration and Privileges

The Configuration Management Administrator and Database Administrator may exercise DDTS administrative procedures to structure DDTS and grant access privileges to DDTS functions. Users who change jobs can be deleted if necessary. The PureSOFT DDTS *Administrator's Manual, Release 3.2*, provides detailed instructions and information about these administrative activities. There are virtually no license restrictions on the number of users who can be granted permission to create and query trouble tickets, or non-conformance reports (NCRs), using DDTS.

It will be necessary to designate someone who will serve as the DDTS administrator. The DDTS administrator will be the owner of the ddts files, and will be authorized to log in as **DDTS**, using a password assigned by the system administrator (**root**). If you are the DDTS administrator, you will be able to configure DDTS so that projects needed for the Testbed are available, with any desired limitations of privileges to those authorized to exercise DDTS functions.

Suppose, for example, that you need to set up a DDTS project to collect NCRs for those who will be responsible for SSI&T. Use the following procedure.

Set Up a DDTS Project

1 On workstation **mss*x*#sun**, at the UNIX prompt in a terminal window, log in using **DDTS** as the login name for the DDTS administrator, and then press the **Enter** key.

- NOTE: The ***x*** in the workstation name will be a letter designating your site: **g** = GSFC, **l** = LaRC, **e** = EDC, and **n** = NSIDC (e.g., **mssn3sun** indicates a management services subsystem Sun workstation at NSIDC). If you access the workstation through a remote login (rlogin), and later wish to run DDTS, you must enter **xhost +** prior to the rlogin, and enter **setenv DISPLAY <local_workstation IP address>:0.0** after the rlogin before entering starting DDTS.
- A **Password:** prompt is displayed.

2 Type the password for the DDTS administrator and then press the **Enter** key.

- The prompt indicates successful login as **DDTS**.

3 Type **adminbug** to start the adminbug program, and then press the **Enter** key.

- The **adminbug>** prompt is displayed.

4 To begin the process for adding a project, type **aprj** and then press the **Enter** key.

- The message **Enter the project name:** is displayed.

5 Type an appropriate name for the project, without spaces (e.g., **LaRC_NCR_SSIT**, **EDC_NCR_SSIT**, **NSIDC_NCR_SSIT**), and then press the **Enter** key.

- The message **Enter a one-line description of the project:** is displayed.

6 Type an appropriate description (e.g., **Collection of NCRs for SSI&T at *site*.** [where ***site*** is a designation for your site, such as **LaRC**, **EDC**, or **NSIDC**]), and then press the **Enter** key.

- The message **Enter project part number:** is displayed.

7 No entry is required for part number; just press the **Enter** key.

- The message **To which class should this project be assigned:** is displayed.

8 Type **software**, and then press the **Enter** key.

- The message **List remote site identifiers for those allowed to modify bugs for this project. A blank line indicates that no remote sites can modify bugs.** is displayed.

9 To restrict use of the project to your site, just press the **Enter** key.

- The message **Inherit parameters from another project? [Y/N]** is displayed.

10 Type **N**, and then press the **Enter** key.

- The message **Enter mail addresses of those to notify upon the arrival of a new bug:** is displayed.

11 Type **DDTS** (the login name of the DDTS administrator) and the login name of anyone else who should be notified (e.g., SSI&T management personnel), and then press the **Enter** key.

- On the Testbed, the login name is sufficient e-mail address. Separate the addresses (login names by a space).
- The message **Enter mail addresses of those to notify when a new bug is assigned to an engineer:** is displayed.

12 Usually, no other users are notified. Just press the **Enter** key. If you want someone notified, type the address(es) (login names) first.

- The message **Enter mail addresses of those to notify when a bug is opened by the assigned engineer:** is displayed.

13 Type the address (login name) of any person to be notified, and/or then press the **Enter** key.

- The message **Enter mail addresses of those to notify when a bug has been resolved:** is displayed.

14 Type the address (login name) of any person to be notified, and/or press the **Enter** key.

- The message **Enter mail addresses of those to notify when a bug has been assigned for verification:** is displayed.

15 Type the address (login name) of any person to be notified, and/or press the **Enter** key.

- The message **Enter mail addresses of those to notify when a bug fix has been verified:** is displayed.

16 Type the address (login name) of any person to be notified, and/or press the **Enter** key.

- The message **Enter mail addresses of those to notify when a bug fix has been postponed:** is displayed.

17 Type the address (login name) of the DDTS administrator, and then press the **Enter** key.

- The message **Enter mail addresses of those to notify when a bug has been declared to be a duplicate of another bug:** is displayed.

18 Type the address (login name) of the DDTS administrator and any other person to be notified (e.g., SSI&T management personnel), and then press the **Enter** key.

- The message **Enter mail addresses of those to notify when a bug has been closed:** is displayed.

19 Type the address (login name) of the DDTS administrator and any other person to be notified (e.g., SSI&T management personnel), and then press the **Enter** key.

- The message **List LOGIN names of those that have project management responsibility:** is displayed.

20 Type the login names of users authorized to make changes to this project's definition, and then press the **Enter** key.

- The message **Are others allowed to subscribe to this project?** is displayed.

21 Type **Y** to enable others to see lists of these SSI&T NCRs, and then press the **Enter** key.

- The message **What Configuration Management System does this project use?** is displayed.

22 Type **clearcase** (note the lack of capitalization), and then press the **Enter** key.

- The message **List LOGIN names of users allowed to ASSIGN-EVAL (A state) a bug. Just hit return if anyone is allowed to ASSIGN-EVAL bugs.** is displayed.

23 Type login names (separated by a space) of those who will be authorized to assign NCRs in this project (SSI&T) for evaluation, and then press the **Enter** key.

- The message **List GROUP names of groups allowed to ASSIGN-EVAL (A state) a bug. Just hit return if any group is allowed to ASSIGN-EVAL bugs.** is displayed.

24 If there are no defined groups, or if any group will be authorized to assign NCRs in this project (SSI&T) for evaluation, just press the **Enter** key. Otherwise, type the group name first.

- The message **List LOGIN names of users allowed to ASSIGN-FIX (O state) a bug. Just hit return if anyone is allowed to ASSIGN-FIX bugs.** is displayed.

25 Type login names (separated by a space) of those who will be authorized to assign NCRs in this project (SSI&T) for fix, and then press the **Enter** key.

- The message **List GROUP names of groups allowed to ASSIGN-FIX (O state) a bug. Just hit return if any group is allowed to ASSIGN-FIX bugs.** is displayed.

26 If there are no defined groups, or if any group will be authorized to assign NCRs in this project (SSI&T) for fix, press the **Enter** key. Otherwise, type the group name first.

- The message **List LOGIN names of users allowed to FIX (R state) a bug. Just hit return if anyone is allowed to FIX bugs.** is displayed.

27 Type login names (separated by a space) of those who will be authorized to perform fixes for NCRs in this project (SSI&T), and then press the **Enter** key.

- The message **List GROUP names of groups allowed to FIX (R state) a bug. Just hit return if any group is allowed to FIX bugs.** is displayed.

28 If there are no defined groups, or if any group will be authorized to perform fixes for NCRs in this project (SSI&T), press the **Enter** key. Otherwise, type the group name first.

- The message **List LOGIN names of users allowed to ASSIGN-VERIFY (T state) a bug. Just hit return if anyone is allowed to ASSIGN-VERIFY bugs.** is displayed.

29 Type login names (separated by a space) of those who will be authorized to assign NCRs in this project (SSI&T) for verification, and then press the **Enter** key.

- The message **List GROUP names of groups allowed to ASSIGN-VERIFY (T state) a bug. Just hit return if any group is allowed to ASSIGN-VERIFY bugs.** is displayed.

30 If there are no defined groups, or if any group will be authorized to assign NCRs in this project (SSI&T) for verification, press the **Enter** key. Otherwise, type the group name first.

- The message **List LOGIN names of users allowed to VERIFY (V state) a bug. Just hit return if anyone is allowed to VERIFY bugs.** is displayed.

31 Type login names (separated by a space) of those who will be authorized to verify NCRs in this project (SSI&T), and then press the **Enter** key.

- The message **List GROUP names of groups allowed to VERIFY (V state) a bug. Just hit return if any group is allowed to VERIFY bugs.** is displayed.

32 If there are no defined groups, or if any group will be authorized to verify NCRs in this project (SSI&T), press the **Enter** key. Otherwise, type the group name first.

- The message **List LOGIN names of users allowed to CLOSE (C state) a bug. Just hit return if anyone is allowed to CLOSE bugs.** is displayed.

33 Type login names (separated by a space) of those who will be authorized to close NCRs in this project (SSI&T), and then press the **Enter** key.

- The message **List GROUP names of groups allowed to CLOSE (C state) a bug. Just hit return if any group is allowed to VERIFY bugs.** is displayed.

34 If there are no defined groups, or if any group will be authorized to close NCRs in this project (SSI&T), press the **Enter** key. Otherwise, type the group name first.

- The message **List LOGIN names of users allowed to declare a bug to be a DUPLICATE (D state). Just hit return if anyone is allowed to declare a bug to be a DUPLICATE.** is displayed.

35 Type login names (separated by a space) of those who will be authorized to declare an NCR in this project (SSI&T) to be a duplicate, and then press the **Enter** key.

- The message **List GROUP names of groups allowed to declare a bug to be a DUPLICATE (D state). Just hit return if any group is allowed to declare a bug to be a DUPLICATE.** is displayed.

36 If there are no defined groups, or if any group will be authorized to declare an NCR in this project (SSI&T) to be a duplicate, press the **Enter** key. Otherwise, type the group name first.

- The message **List LOGIN names of users allowed to POSTPONE (P state) a bug. Just hit return if anyone is allowed to POSTPONE bugs.** is displayed.

37 Type login names (separated by a space) of those who will be authorized to postpone NCRs in this project (SSI&T), and then press the **Enter** key.

- The message **List GROUP names of groups allowed to POSTPONE (P state) a bug. Just hit return if any group is allowed to POSTPONE bugs.** is displayed.

38 If there are no defined groups, or if any group will be authorized to postpone NCRs in this project (SSI&T), press the **Enter** key. Otherwise, type the group name first.

- The message **List LOGIN names of users allowed to view a bug. Just hit return if anyone is allowed to view bugs.** is displayed.

39 Type login names (separated by a space) of those who will be authorized to view NCRs in this project (SSI&T), and then press the **Enter** key.

- The message **List GROUP names of groups allowed to view a bug. Just hit return if any group is allowed to view bugs.** is displayed.

40 If there are no defined groups, or if any group will be authorized to view NCRs in this project (SSI&T), press the **Enter** key. Otherwise, type the group name first.

- The **adminbug>** prompt is displayed.

41 Type **quit** to quit the adminbug program.

- The prompt for the DDTS administrator is displayed.

Adding Users to DDTS

A person provided with a new account on the system and authorized access to DDTS is automatically able to use projects to the extent that restrictions are not placed on functions. If certain functions are restricted to a specified set of users or groups, and if the person with the new account is to be authorized access to a restricted function, it will be necessary to modify the project to permit the access. Use the following procedure.

Adding a User to a DDTS Project

1 On workstation **mss*x*#sun**, at the UNIX prompt in a terminal window, log in using **DDTS** as the login name for the DDTS administrator, and then press the **Enter** key.

- NOTE: The ***x*** in the workstation name will be a letter designating your site: **g** = GSFC, **l** = LaRC, **e** = EDC, and **n** = NSIDC (e.g., **mssn3sun** indicates a management services subsystem Sun workstation at NSIDC). If you access the workstation through a remote login (rlogin), and later wish to run DDTS, you must enter **xhost +** prior to the rlogin, and enter **setenv DISPLAY <local_workstation IP address>:0.0** after the rlogin before entering starting DDTS.
- A **Password:** prompt is displayed.

2 Type the password for the DDTS administrator and then press the **Enter** key.

- The prompt indicates successful login as **DDTS**.

3 Type **adminbug** to start the adminbug program, and then press the **Enter** key.

- The **adminbug>** prompt is displayed.

4 To begin the process for modifying the project, type **mprj** and then press the **Enter** key.

- The message **Enter the project name:** is displayed.

5 Type the name of the project to be modified (e.g., **EDC_NCR_SSIT**), and then press the **Enter** key.

- The message **Enter a one-line description of project:** is displayed, along with the previously entered description which may be edited.

6 Press the **Enter** key to cycle through the project fields, repeating the press until you reach a field where you need to add the new user to grant access to a restricted function.

- The message prompt for the field is displayed, along with the previously entered information that established the restriction.

7 Edit the displayed information, adding the login name of the new user, and then press the **Enter** key.

- The message prompt for the next field, along with its previously entered information, is displayed.

8 Repeat **Steps 6** and **7** until you have added the new user's login name wherever necessary to grant the desired access, and until you reach the end of the fields for the project.

- The **adminbug>** prompt is displayed.

9 Type **quit** to quit the adminbug program.

- The prompt for the DDTS administrator is displayed.

Performing Operational Work-around

An operational work-around is a temporary modification to operations and user procedures that is entailed by resolution of a trouble ticket. It is characterized by several factors that may affect the way in which procedures are accomplished to conduct operations during the period of temporary inability to conduct operations using normal procedures:

- managed by the ECS Operations Coordinator at each center.
- master list of work-arounds and associated trouble tickets and configuration change requests (CCRs) kept in either hard-copy or soft-copy form for the operations staff.
- hard-copy and soft-copy procedure documents are “red-lined” for use by the operations staff.
- work-arounds affecting multiple sites are coordinated by the ECS organizations and monitored by ECS M&O Office staff.

The work-around is removed when the CCR that corrects the original problem is installed into the operational baseline.

Diagnosing Network Communications Problems

Network problems or faults are failures occurring within the network that prevent the network from meeting its operational objectives. Just as with other problems, management of network faults requires:

- detection of the fault.
- isolation of the fault.
- correction of the fault.

The elements of troubleshooting that support diagnosis of network communications problems are, therefore, essentially the same as those that support other fault diagnosis, and the tools you have learned about for system performance monitoring and troubleshooting are applicable:

- error logs.
- error detection processes.
- diagnostic testing.

Identifying Network Connectivity Problems

Network connectivity problems are indicated by a variety of possible symptoms. These include:

- a user's inability to contact a particular system (e.g., through remote login or file transfer protocol) that had been accessible in the past.
- receipt of an error message that the connection timed out, which could be caused by a system being down, a routing problem, a problem on the default gateway, or bad performance on the network preventing packets from timely passage.
- receipt of an error message indicating an error that the remote system could not be found (e.g., perhaps it is shut off, or it is no longer on the network).

As we have seen, the HP OpenView monitoring tool provides a quick way to detect and identify problems in a network. Its color maps include warnings and indications of major and critical problems with the operational status of elements in the network, including connections between nodes. Therefore, the procedure for looking at HP OpenView network maps for color alerts can help you identify network connectivity problems. If a user or operator is unable to connect to a remote system, a quick check for color alerts can tell you if that system is down. It can also be important to pay attention to the colors of the lines on the map indicating network connections. If you use the HP OpenView default status colors (see Figure 2 on page 8), problems of increasing severity are indicated by a progression of colors as follows:

- cyan -- warning; system faces a potential problem.
- yellow – minor; there is a problem not immediately impeding normal use.
- orange – major; there is a serious problem likely to impede normal use.

- red – critical; there is a severe problem and the affected element is not functioning.

When an operator/user is having problems connecting from one system to another within the same network, a further check for connectivity can be made using HP OpenView Network Node Manager (NNM) and the following procedure to **Ping** the remote system.

Diagnosing Connectivity Problems within a Network

1 On the network map, click on the icon for the remote system.

- The selected icon is highlighted.

2 Follow menu path **Fault→Ping**.

- A window is displayed to show repeated pings. If the remote system is down, the ping will fail. If the ping is successful, repeat steps 1 and 2 for the operator's/user's system (from which the connection was originally attempted). If the ping to either system fails, go to step 5. If the ping to both systems is successful, go to step 3.

3 On the network map, click on the icon for the operator's/user's originating system, and then click on the icon for the remote system while holding down the **Control** key.

- Both systems are highlighted.

4 Follow menu path **Fault→Remote Ping**.

- A window is displayed to show repeated pings from the originating system to the remote system. If the ping fails, go to step 5. If it is successful, the problem may be in the address mapping between the originating system and the remote system. This can be verified and corrected by using **nslookup** (from a terminal window) to compare the IP address-to-hostname mapping service and IP address for the remote system as seen by the originating system and as it actually is (as seen by another source system).

5 Finally, check for any IP address-to-link address mapping problems by comparing the **Link Address** for the remote system as it is set in the originating system and as it is set in one which is able to communicate with the remote system. To achieve this, select on the map the originating system and also your system. Then, to view the Address Resolution Protocol Cache (ARP Cache) table, follow menu path **Configuration→Network Configuration→ARP Cache**.

- The **ARP Cache** window is displayed for each system selected on the map.
- In the displayed list for the originating system, find the IP Address for the remote system and note its **Link Address**. In the **ARP Cache** window for your workstation, find the IP Address for the remote system in the list and compare its **Link Address** with the one shown in the list for the originating system. If they are not the same, it will be necessary to fix the remote system's link-level address on the originating system. If they are the same, it may be necessary to look for something other than a connectivity problem.

If an operator/user is having difficulty in connecting from a system on one network to a system on a different network, the procedure is somewhat different. If a check of the network map for color alerts determines that the remote system is not down, use the Network Node Manager and the following procedure for further analysis.

Diagnosing Connectivity across Networks

1 On the network map, click on the icon for the remote system.

- The selected icon is highlighted.

2 Follow menu path **Fault→Ping**.

- A window is displayed to show repeated pings. If the remote system or its gateway is down, the ping will fail. If the ping is successful, repeat steps 1 and 2 for the operator's/user's system (from which the connection was originally attempted). If that ping is successful, go to step 5. If the ping to either system fails, go to step 3.

3 On the network map, click on the icon for the gateway to the network with the system for which the ping failed.

- The selected icon is highlighted.

4 Follow menu path **Fault→Ping**.

- A window is displayed to show repeated pings. If the gateway is down, the ping will fail. If the ping is successful, the system for which the ping failed in step 2 is down.

5 On the network map, click on the icon for the operator's/user's originating system, and then click on the icon for the remote system while holding down the **Control** key.

- Both systems are highlighted.

6 Follow menu path **Fault→Locate Route: via SNMP**.

- On the map, the path between the selected systems is highlighted and a window is displayed listing for each node the **Source**, **Source Address**, **Next Hop**, and **Next Hop Address**.
- Verify that the highlighted path is correct; if the route leads to a system other than the one selected, the routing table for the originating system is incorrect. You can view the routing table for each node in turn by clicking on it and then following menu path **Configuration→Network Configuration→Routing Table**.

7 Observe the map to verify that all nodes along the correct path are up. A node with yellow or red status indicates that the node either has a problem or is down. If the icon for a node is yellow or red, you need to diagnose the problem on that node.

- If the route is correct and everything is up along the path, it may be necessary to look for something other than a connectivity problem.

Identifying Network Performance Problems

Network performance is more than just a matter of whether the network is functioning or not. Asking whether "normal use" is impeded or not implies an assessment of what is "normal." If there is a slowdown in the speed of a transaction on the network, perhaps because of high demand, such as an unusually high number of requests being placed on the Science Data Server, users may make a subjective judgment that the performance is not normal. Performance management involves gathering statistics on the operation of the network, maintaining and analyzing logs of the state of the system, and optimizing network operation. If a user concern about the functioning of the system results in a trouble ticket addressing an apparent degradation in the performance of the network, a tools that may help operators/maintainers identify a network performance problem is:

- HP OpenView – permits use of a menu path (e.g., **Performance→CPU Load**, **Performance→Graph SNMP Data→Selected Nodes . . .**) to obtain graphical displays of system performance measures (e.g., interface traffic, CPU usage) on a time line (see example in Figure 5).

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Time	CPU Utilization											
2	8:00	1											
3	8:15	9											
4	8:30	15											
5	8:46	26											
6	9:02	27											
7	9:15	26											
8	9:30	32											
9	9:45	28											
10	10:01	31											
11	10:16	28											
12	10:31	31											
13	10:45	29											
14	11:01	27											
15	11:16	22											
16	11:31	26											
17	11:46	21											
18	12:01	22											
19	12:16	16											
20	12:32	17											
21	12:46	13											
22	13:02	17											
23	13:16	12											
24	13:30	10											
25	13:45	7											
26	14:01	9											
27	14:15	5											
28	14:31	6											
29	14:45	3											
30	15:01	4											
31	15:16	5											
32	15:30	3											
33	15:47	2											
34	16:01	3											
35	16:16	1											
36	16:30	0											
37	16:47	0											

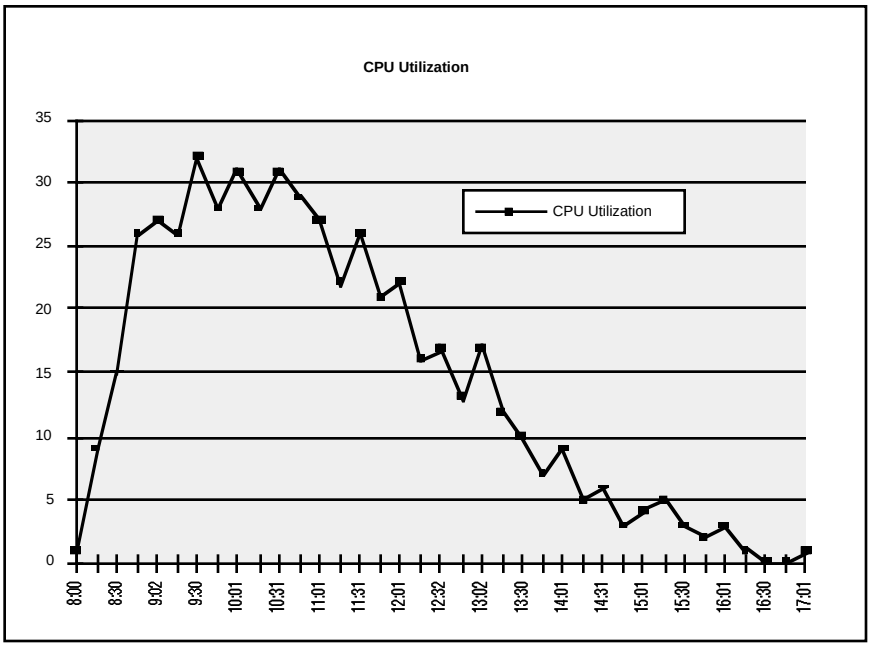


Figure 5. Example of HP OpenView Graphical Display of CPU Usage

Diagnosing Network Service Problems

Sometimes it is possible for an operator/user to connect to a remote system, but a command to the remote system is not accepted. For example, a user may try to use a network service (e.g., ftp) from a system on one network to a system on another network, but get an error message. In troubleshooting this problem, the following procedure is applicable.

Diagnosing Network Service Problems

1 On the network map, click on the icon for the remote system.

- The selected icon is highlighted.

2 Follow menu path **Fault→Test IP / TCP / SNMP** to make sure that the selected system supports the network protocols and that the protocols are working.

- A window is displayed to show the results of the test. If there are problems with the protocol, an error will appear in the messages field of the window.
- If the test shows OK, repeat steps 1 and 2 for the originating system. If both systems check out OK, go to step 3.

3 On the network map, click on the icon for the remote system.

- The selected icon is highlighted.

4 Follow menu path **Configuration→Network Configuration→Services** to make sure that the selected system supports the service in question (e.g., **ftp**).

- A window is displayed to show the following information about the selected node:
  - the service protocol: either TCP (Transmission Control Protocol) or UDP (User Datagram Protocol).
  - The port to which the service is bound.
  - The service for which the node is listening (e.g., **ftp**, **telnet**).
- If the test shows OK, repeat steps 1 and 2 for the originating system. If both systems support the service in question, go to step 5. If not, do the following:
  a) Check the file system on the two systems to see if the software for the service (e.g., ARPA Services) is installed. If not, you will have to install the software on the system. If the service software is installed, go to step b.
  b) Configure the service (e.g., ARPA Services) on the system. For HP-UX systems using SAM (System Administration Manager), use the menu path **Configure→HP-UX SAM . . .** to access the SAM tool to configure the service.
  c) Skip step 5 and go to step 6.

5 Check service security on the remote system. Make sure the IP address of the originating system is set for "allow access" and not excluded by a "deny access" in the security files for the service in question (e.g., **/usr/adm/inetd.sec** and **/etc/ftpusers**).

6 Try to use the service again, from the originating system to the remote system, to verify that the problem is resolved.

If there is a problem with network service or performance and you are assigned to work on the trouble ticket, your approach should be a series of systematic steps to diagnose the problem. The steps include:

1. *Review the information in the trouble ticket*. The review gives you insight into the nature of the service problem. For example, if a user experiences a delay in service, such as an apparently too long delay during a request to browse a specified data product using the Search and Order Tool, the description on the trouble ticket describes this system behavior.
2. *Use HP OpenView to see if an alarm has been triggered*. Look for color alerts, and if possible isolate the problem to a particular area of the network.
3. *Use other HP OpenView functions to assist in isolating the problem*. If it is not possible to determine the problem area through color alerts, follow menu path **Locate→Objects** to bring up the map containing a relevant host. For example, review of the trouble ticket for the sample problem mentioned in Step 1 tells you that the problem is with the Science Data Server (SDS), which you know is necessary for a user to browse a specific data product. Using the menu path **Locate→Objects→By Selection Name . . .** can bring up the map containing the SDS managed host.
4. *Use HP OpenView to check the network activity on the host*. Follow menu path **Performance→Network Activity→Interface Traffic**. HP Open View displays an "Interface Traffic" graph containing packets received, packets transmitted, errors received, and errors transmitted. In the sample problem mentioned in Step 1, it is quite possible that the network activity dies not show any sign-on problems or an unacceptable level of activity.
5. *Use HP OpenView to check the CPU load on the host*. Select the managed host (in our example, the SDS host), and follow menu path **Performance→CPU Load**. HP Open View displays a "CPU Load" graph containing the average CPU load on that host. Follow menu path **View→Time Intervals** to bring up a control dialog and scroll back to the time period reported on the trouble ticket for the problem. If there were unusually high numbers of requests during that time period, the CPU Load graph should reflect that high demand. Note, however, that just seeing a high CPU load does not tell you its cause.

Viewing Historical Trends

One of the most useful sources of network troubleshooting information is the history of events leading up to and associated with a problem. To be able to review a history of events, it is necessary to take a proactive view of the system and ensure that data on significant events are monitored and logged. The HP OpenView tool Network Node Manager provides several capabilities to facilitate proactive monitoring of the network, including:

- data collection.
- event configuration.
- application building (for applications to do the monitoring).

The initial set-up or full configuration for effective monitoring of the network can require several weeks to achieve, but it is well worth the attention required to establish a monitoring approach that will require little from you to administer but will provide useful troubleshooting data when it is needed. The set-up process for monitoring with HP OpenView entails several steps which you will want to accomplish in the first few weeks of your network management activities:

- establish baselines for normal network performance.
- build applications to monitor trends.
- set up thresholds for monitored Management Information Base (MIB) values.
- refine the thresholds.
- set up event-triggered actions.

Establishing Baselines for Normal Network Performance

Establishing a baseline requires checking the condition of the network over a period of time. To accomplish this, it is necessary to select information to look at, and then monitor it during the course of several days or weeks. Suppose, for example, that you are interested in the Maintenance and Operations segment and wish to collect data on the SSI&T Workstations. The following procedure is applicable.

Establishing Baselines for Normal Network Performance

1 Follow menu path **Options→Data Collection & Thresholds: SNMP**.

- A dialog box titled **is Data Collection & Thresholds: SNMP** is displayed.
- If the MIB object on which you want to collect data is already displayed in the **MIB Objects** list in the dialog box, click on that object. [NOTE: The enterprise-specific Management Information Base (MIB) for which you want to collect data must be loaded into the Loaded MIB database. For ECS installations, this has been done for you, and the objects will appear. If a new object has been added to the network, and you want to collect data on it, see *HP OpenView, Using Network Node Manager*, "Loading MIBs" in the chapter on Managing MIB Data.] For this example, if you are interested in monitoring traffic on the hub and printer nodes, you may wish to monitor the following MIB objects:

- **.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets**.
- **.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets**.

2 Click on **.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets** and then follow menu path **Edit→Add→MIB Collections**.

- The **Data Collection & Thresholds/Add Collection for *xxxxx*** dialog box is displayed.

3 Add the source name (the name or IP address of the node on which you want to collect data), either by entering the name in the **Source** field and clicking on the **Add** button, or by selecting the node(s) (for this example, select the AIT workstations) on the network map and clicking on the **Add From Map** button.

- The **List of Collection Sources** list area shows the name(s) of the selected node(s).
- Repeat this step to add other names to the **List of Collection Sources** as desired.

4 Specify the collection mode using the **Collection Mode** option button and choosing one option from its option menu.

- The four choices on the **Collection Mode** option menu are "**Exclude Collection**" (a way of excluding certain devices from a wildcard list, which may be specified in Step 3), "**Store, Check Thresholds**," "**Store, No Thresholds**," and "**Don't Store, Check Thresholds**." For example, select "**Store, No Thresholds**."

5 Specify a polling interval in the **Polling Interval** field by entering a positive real number followed by an "**s**," "**m**," "**h**," "**d**," "**w**," or "**y**," indicating seconds, minutes, hours, days, weeks, or years, respectively. For example, enter "**1h**" to poll at hourly intervals.

WARNING

A collection with a short polling interval can easily fill up a disk. Be aware of the current collection configuration.

6 Specify the MIB instance of the object on which you want to collect data. To do this, click on the option button and select the **All** option.

- The options are "**All**" instances of the MIB object, "**From List**" as specified in the input box, and "**From Regular Expression**" as specified in the input box.

7 Click on the **OK** button. The **Data Collection & Thresholds/Add Collection** dialog box disappears and the MIB object(s) is/are added to the selection list of MIB objects configured for collection in the **MIB Data Collection** dialog box.

8 Repeat steps 2 through 7, except in step 2 click on **.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets**.

9 Check to see if data are being collected by observing the status (**Collecting** or **Suspended**) listed in the **MIB Data Collection** dialog box.

- If the status of the MIB object(s) is **Suspended**, change it to collecting by selecting (highlighting) the object(s) and following menu path **Actions→Resume Collection**.

10 Implement the change and begin collection by following menu path **File→Save**.

NOTE: Even though the status entry shows a change when you follow menu path **Actions→Resume Collection**, the change does not take effect until you perform the **File→Save** operation.

Building Applications to Monitor Trends

You can use HP OpenView to build applications without programming to display collected MIB data. These applications can be integrated into the HP OpenView menu structure for ease of use. For example, to graph the data collected on your selected workstations, the following procedure is applicable.

Building an Application to Monitor Trends

1 Follow menu path **Options→MIB Application Builder: SNMP**.

- The **MIB Application Builder:SNMP** dialog box is displayed.

2 Follow menu path **Edit→Add MIB Application . . . .**

- The **Add MIB Application** dialog box is displayed.

3 Type the name of the application (e.g., in this case, **SSTraffic**) in the **Application ID** field.

- This field determines the name of the file where the application information is to be stored (in the $OV_REGISTRATION/C/ovmib/ directory); therefore, each application must have a unique name.

4 Select the type of application you want to build by clicking on the **Application Type** option button.

- There are three options for application type: **Form**, **Table**, and **Graph**. For this example, select **Graph**.

5 Enter the title of your application (e.g., **SSIT Traffic**) in the **Application Title** field.

- This title appears in the menu path (e.g., **Performance→Graph SNMP Data→ SSIT Traffic**) and in the title bar of the dialog box when the application is run.

6 Click on the **Add** button of the **Add MIB Application** dialog box.

- The **MIB Application Builder/Add MIB Objects** dialog is displayed.

7 Specify the MIB object to include in your application (in this case, **.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets**).

- The specification may be done in either of two ways: 1) navigate the MIB tree and select the desired object, or 2) type in the MIB object in the **MIB Object ID** field.

8 Click on the **Apply** button.

- The MIB object is added to the **Display Fields** window of the **Add MIB Application** dialog box and the **MIB Application Builder/Add MIB Objects** dialog box remains displayed.

9 Repeat Steps 7 and 8 to specify additional MIB objects to include in your application (in this case, **.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets**).

- In Step 8, after the specification of the last MIB object to be included, you may click on the **OK** button (instead of the **Apply** button). In this case, the MIB object is added to the **Display Fields** window of the **Add MIB Application** dialog box and the **MIB Application Builder/ Add MIB Objects** dialog box is closed. If you do not use the **OK** button, when finished you will have to exit the **MIB Application Builder/ Add MIB Objects** dialog box by clicking on the **Cancel** button.

10 Optionally, edit the **Label** for each MIB object selected.

- The default is the last component of the MIB object name; when a MIB object in the **Display Fields** window is highlighted, this last component appears in the **Label** field, where you may edit it and implement the edits by clicking on the **Replace** button.

11 Optionally, change the order of the items in the list by selecting an item to move and clicking on the **Up** or **Down** arrows to the right of the **MIB Object ID** list; each click moves the item up or down one position.

- Changing the order affects the order in which the items are displayed when you run the application.

12 To make the application appear in the HP OpenView menu hierarchy, enter the menu path in the **Menu Path** input box of the **Add MIB Application** dialog box.

- Use the character sequence -> to separate menu items in the cascaded path.

13 Enter the OVW selection rule in the **Selection Rule** field.

- The default selection rule is based on defined HP OpenView capabilities of the nodes for which the application is compatible; components of the rule are separated by "||" to indicate logical "or" or "&&" to indicate logical "and."

- If the application is registered in the menu bar (Step 12), the menu item for this application is only accessible if the capabilities of the selected nodes match those defined in this selection rule. For our example, if the selection rule is specified as **(isSNMPsupported)||(is SNMPProxied)&&(isNode)&&isWorkstation)**, then the menu choice will be grayed out unless the selected node is a workstation that is SNMP supported or proxied.

14 Enter any help text that you want displayed for your application.

- When you create the MIB operation menu item, the program automatically adds an entry accessible through menu path **Help→Index→Function** and in the dialog box accessible by clicking on the **Help** button.

15 Click on the **OK** button.

- The new MIB application is created and the **Add MIB Application** dialog box is closed.

Once you have collected data for a suitable period of time to observe trends (e.g., two weeks), you can review the data. One powerful tool for viewing historical data is the HP OpenView Grapher. We have already seen an example of using an HP OpenView graph, *viz.*, to view CPU load. The HP OpenView Grapher assists the review of historical trends in several ways, permitting:

- the organization and viewing of collected information in graph form.
- the graphing of combinations of data values in the same graph.
- viewing data values representing different instances of data variables or different variables for different nodes.
- viewing data for selected nodes or viewing all the data in the Data Collector database.

Before accessing the Grapher, data collection on the nodes of interest must have been started by using menu path **Options→SNMP Data Collection & Thresholds**, as just described. Then, when the Grapher is started, all the collected data from the selected nodes will be read into memory and will be available for browsing with the Grapher functions, using the following procedure.

Viewing Historical Trends using HP OpenView Grapher

1 On the network map, click on the icon(s) for the node(s) of interest.

- The selected icon is highlighted.

2 Follow menu path **Performance→Graph SNMP Data→Selected Nodes**.

- The primary window for the HP OpenView Graph tool is displayed.
- The **Graph Selected Nodes** dialog box is displayed. It is a line graph with a legend across the top of the graph to identify the graphed data and time shown on the X-axis.

3 Manipulate the graph to obtain the desired display.

- Available manipulations include **selecting time intervals**, **zoom, modifying line attributes**, and **resizing the graph window**.

After you have collected and reviewed data for a period of time, you may wish to define thresholds for monitored numeric MIB values. This permits you to set limits on the collection of data such that an event record is made only when the monitored value exceeds established boundary conditions. Suppose, for example, that you have monitored and reviewed traffic on the hub for two weeks, and you believe that the traffic during that time is representative of typical traffic during normal operations. You note the maximum value for inbound octets (**ifInOctets**) during that period, and decide that for monitoring hub traffic you want to have an event recorded only if that value is exceeded. You want to set the threshold at that level, and to set a rearm value of 10 percent of the threshold value. (NOTE: The rearm value controls how frequently a threshold event is generated by the data collector. When the MIB value satisfies the **Rearm** expression, a rearm event is generated. Another threshold event will not be generated until the rearm event occurs and the collected value subsequently satisfies the **Threshold** expression.) The following procedure is used.

Defining Thresholds and Rearm Values

1 Follow menu path **Options→Data Collection & Thresholds: SNMP**.

- A dialog box its title is **Data Collection & Thresholds: SNMP** is displayed.

2 From the **MIB Objects Configured for Collection** selection list, select the item for which you want to set thresholds.

- The details for that item appear in the lower section of the dialog box, **MIB Collection Summary**.

3 Select the source from the **MIB Collection Summary** list.

- You may select multiple items.

4 Follow menu path **Edit→Modify→MIB Collections**.

- The **Data Collection & Thresholds, Modify Collection** dialog box is displayed.

5 Select either **Don't Store, Check Thresholds** or **Store, Check Thresholds** from the option menu next to the Collection Mode label.

- The **Threshold** and **Rearm** fields are un-grayed and made available.

6 Specify a polling interval in the **Polling Interval** field by entering a positive real number followed by an "**s**," "**m**," "**h**," "**d**," "**w**," or "**y**," indicating seconds, minutes, hours, days, weeks, or years, respectively. For example, enter "**1h**" to poll at hourly intervals.

WARNING

A collection with a short polling interval can easily fill up a disk. Be aware of the current collection configuration.

7 Specify a **Specific Event** (i.e., trap) number.

- The default **Specific Event** (58720263) is the enterprise-specific trap that the data collector sends when a threshold or rearm value is exceeded. When you are customizing a data collection, you can assign your own trap number, using an odd number between 1001 and 1999. (The even numbers 1002 to 2000 are reserved for the respective rearm trap IDs, which are generated automatically by HP Open View.) For this example, specify **1901** as the trap number.
- The data collector sends the trap using the Enterprise ID of the Management Station.
- The default trap is logged in the **Threshold Events** category in the **Events** notification window.
- The exact trap number allows you to perform a specific action when this kind of threshold value is passed or rearmed.

8 Enter the threshold value (in this case, ***TBD***) in the **Threshold** field.

- Use this field when you want to be notified of data patterns that are outside normal expectations. When the threshold value is passed, the specified event is generated, and the **Event Categories** window notifies you accordingly.

9 Enter a rearm value (in this case, ***TBD***) in the **Rearm** field and click on the appropriate toggle button to specify whether the entered value is **Absolute** or a **Percent** of the threshold value.

- The **Rearm** value is used to avoid continuous generation of events while a collected value exceeds the threshold value. When the MIB Object value drops below, or is equal to, the **Rearm** value, a **Rearm Event** is generated. Another **Threshold Event** will not occur until the **Rearm Event** is generated and the MIV Object value again exceeds the threshold setting.

10 Optionally, specify a value for the **Consecutive Samples** field.

- This value specifies the number of consecutive times the **Threshold** expression must be satisfied before a corresponding event is generated.

11 Specify on which instance of the MIB Object you want to collect data.

12 Click on the **Apply** button to remain in the dialog box, or click on the **OK** button which will exit the **Data Collection & Thresholds** dialog box.

- The new collection parameters are initiated.

Refining Thresholds

Once you have monitored your system for a time using thresholds, you will have a basis for assessing the appropriateness of the thresholds you set. You may note one of at least two possible conditions that suggest resetting the threshold and rearm values:

- you are receiving several threshold events in the course of a day without any apparent loss in network performance (e.g., hub traffic is high enough to exceed the set thresholds, but everyone finds their printing needs satisfied without trouble).
- you are experiencing network performance problems but are not receiving threshold events that might give you advance warning of those problems (e.g., there are large backlogs that cause people to have to wait excessively long for print jobs, but the hub and printer traffic are not sufficient to cause threshold events).

To refine your thresholds, the following procedure is applicable.

Refining Thresholds for MIB Data Collection

1 On the map, select the node for which you want to change the threshold/rearm value (e.g., select the printer hub).

2 Follow menu path **Options→Data Collection & Thresholds: SNMP**.

- The **MIB Data Collection** dialog box appears (its title is **Data Collection & Thresholds: SNMP**).

3 From the **MIB Objects Configured for Collection** selection list, select the item for which you want to reset thresholds.

- The details for that item appear in the lower section of the dialog box, **MIB Collection Summary**.

4 Select the source from the **MIB Collection Summary** list.

- You may select multiple items.

5 Follow menu path **Edit→Modify→MIB Collections**.

- The **Data Collection & Thresholds, Modify Collection** dialog box is displayed.

6 Enter the new threshold value (in this case, ***TBD***) in the **Threshold** field.

- When the threshold value is passed, the specified event is generated, and the **Event Categories** window notifies you accordingly.

7 Enter a rearm value (in this case, ***TBD***) in the **Rearm** field and click on the appropriate toggle button to specify whether the entered value is **Absolute** or a **Percent** of the threshold value.

- When the MIB Object value drops below, or is equal to, the **Rearm** value, a **Rearm Event** is generated. Another **Threshold Event** will not occur until the **Rearm Event** is generated and the MIV Object value again exceeds the threshold setting.

8 Optionally, once you have fine tuned the threshold settings, you may want to turn off the data storage function, but continue to check for thresholds. To do this set the data collection mode to **Don't Store, Check Thresholds** by selecting that option from the option menu next to the Collection Mode label.

9 Click on the **Apply** button to remain in the dialog box, or click on the **OK** button which will exit the **Data Collection & Thresholds** dialog box.

- The new collection parameters are initiated.

Setting Up Event-Triggered Actions

Once you have attained stability in threshold settings, you may find it desirable to set up an action to occur when one of the threshold values is exceeded. For example, you may wish to have a pop-up window appear to notify you with a message and, perhaps, with an audible signal upon occurrence of SSI&T Workstation traffic in excess of your set threshold. Use the following procedure.

Event Configuration

1 Open the **Event Configuration** dialog box by following menu path **Options→Event Configuration**.

- The **Event Configuration** dialog box is displayed.

2 Select the item in the **Enterprise Identification** list which corresponds to the event you want to configure (e.g., select SNMP).

- Defined events for that Enterprise Identification appear in the **Event Identification** list.

3 Follow menu path **Edit→Add→Event**.

- The **Event Identification/Add Event** dialog box is displayed.

4 Enter a unique event name (this name cannot contain embedded spaces) in the **Event Name** field (e.g., enter **SSIT_High** to indicate SSI&T Workstation Traffic High).

5 Use the option button and associated menu to select the generic trap type. For this example, select **Enterprise Specific**.

6 In the **Specific Trap** field, which is displayed only when you have selected the **Enterprise Specific** option for generic trap type, enter the specific number of the trap.

- In this case, specify **1901** (The trap ID you choose here must be the same as the one you set up in the data collection and threshold specification).

7 In the **Event Description** field, enter any text description you want to provide to characterize the meaning of the event.

8 In the **Event Sources** field, enter the sources (nodes) for which the event applies, or select the sources on the map and click on the **Add from Map** button.

9 Use the **Event Category** option button to select the category in which to display notification of the event.

- Select **Threshold Events**. If you select "Log Only" or "Don't Log or Display," the event will not be displayed in the Event Log Browser.

10 Use the **Severity** option button to select the severity of the event.

- For this example, select **Warning** as the severity level appropriate for exceeding the threshold.

11 In the **Event Log Message** field, leave the default message. This message will appear in the event notification window when the event is received.

12 In the **Popup Notification** field, type the message which you want to appear in the popup window when the event occurs (e.g., "**SSI&T traffic threshold exceeded; check Event Log Browser for details.**").

12 Leave the **Command** field blank. This field can be used to specify a command and corresponding arguments to be performed automatically upon occurrence of the event.

13 Follow menu path **File→Save** and save the event.

Using the Event History Log Browser

Another ECS tool of use for reviewing events at or near the time of a problem is HP OpenView **Event History Log Browser**. When a popup notification is received, or to review details of events indicated by a color alert in the HP OpenView **Event Categories** window, you can examine the listings in this browser. To use this HP OpenView tool, select the managed host (e.g., the SSI&T host) and enter the initial time to be near, but prior to, the time the problem is known to have occurred. Use the following procedure.

Using HP OpenView Event History Log Browser

1 Follow menu path **Fault→Event**.

- The **All Events Browser** window is displayed.

2 Follow menu path **View→Set Filters . . . .**

- The **Filters** window is displayed.

3 Click on the toggle button for **Match By Time**.

- A time **scroll bar** appears: use the slider to set the initial time.

4 On the network map, click on the managed host (e.g., **aitx1sun**).

- The selected icon is highlighted.

5 Click on the toggle button for **Match Source**.

- A source **text window** appears with text entry field and buttons.

6 Click on the **Add From Map** button.

- The source identifier appears in the text window.

7 Click on the **Apply** button.

- The Event History Log Browser displays the events from **aitx1sun** in the selected time period.

Practical Exercise

Introduction

This exercise is designed to practice key elements of the System Troubleshooting procedures. Perform the tasks identified in the exercise.

Equipment and Materials

One ECS workstation.

Perform Activities Related to System Monitoring and Troubleshooting

1. Use ECS tools to perform system monitoring activities, including HP OpenView maps and event log files for checking the health and status of the network and the web browser to access the EBnet Web Page.
2. Use HP OpenView to check for event notifications, and browse the event logs for several event categories as you would to diagnose a problem event.
3. Set up a new project for DDTS. Then add a user to the list of those to be notified when a bug has been declared to be a duplicate of another bug.
4. Use HP OpenView Network Node Manager and configure the system to collect data on a network node, using thresholds and rearm values.

This page intentionally left blank.

Slide Presentation

Slide Presentation Description

The following slide presentation represents the slides used by the instructor during the conduct of this lesson.